The Lloyd Williamson Nurseries

E-Safety Policy: Bring Your Own Device (BYOD) Policy for Staff and Visitors

2025-2026

Updated by Lucy Meyer
Date: 01.10.25
Due for Update: September 2026

Introduction

The Lloyd Williamson Nurseries recognises that tablets offer valuable benefits to staff from an observation and learning perspective. Our nurseries require that they are only used for specific purposes i.e. observations on Tapestry.

This policy is intended to address the use of personal devices by staff members and visitors to then nurseries.
These devices include (but aren't limited to) smart phones, tablets, laptops, wearable technology and any similar devices. If you are unsure whether your device is captured by this policy please check with the nurseries' management.
These devices are referred to as 'mobile devices' in this policy.
Sections one, two and four of this policy apply to all nursery staff and to visitors to the school. The rest of the policy is only relevant to nursery staff.

Policy statements

1. Use of mobile devices at the nurseries

Staff must only use mobile devices in the staff room, during free time. Mobile devices may not be checked during working hours.
Visitors to the school may use their own mobile devices in the following locations:

- In the staff room
- Visitors mobile devices should be handed in prior to entering the nursery rooms. With consent, they may use the devices for specific reasons e.g. Ofsted but not in any space/room where children are present.

Staff and visitors to the school are responsible for their mobile device at all times. The school is not responsible for the loss, or theft of, or damage to the mobile device or storage media on the device (e.g. removable memory card) howsoever caused. The office must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged by management.
Mobile devices must be turned off whilst in the building unless in use in a designated area and or at a specifies time (e.g. lunch breaks) and must not be taken into any other areas of the nurseries.
The nurseries reserve the right to refuse staff and visitors permission to use their own mobile devices on nursery premises.
Please note smart watches or any device which can record or send messages are not allowed at the nurseries.

2. Access to the school's Internet connection

The school provides a wireless network that staff and visitors to the nurseries may use to connect their mobile devices to the Internet. Access to the wireless network is at the discretion of the nurseries, and the nurseries may withdraw access from anyone it considers is using the network inappropriately.
The nurseries cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. In particular, staff and visitors are advised not to use

the wireless network for any personal us such as online banking or shopping.
The nurseries are not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the nurseries' wireless network. This activity is taken at the owner's own risk and is discouraged. The nurseries will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the nurseries' wireless network.

3. Access to the nurseries' IT services

All nursery staff are allowed to connect to or access the following school IT services from their mobile devices:

- The nurseries' e-mail webmail
- Specific online learning such as Educare

Staff must only use the IT services listed above (and any information accessed through them) for work purposes.
Staff must not send nursery information e.g. emails to their personal email accounts.

4. Monitoring the use of computers

Staff must request to use the nurseries' computers – this should be for a specified reason e.g. printing checklists. In normal circumstances, there is no reason to use them. Computers may not be used for personal reasons e.g. personal emails/shopping etc.

Staff have access to tablets for the sole use of observations through Tapestry. Any other use must be agreed by the SMT prior to use.

Staff may not use their own computers on nursery property without permission from the SMT and then they should only be used for training purposes or to access work emails. They may not be used outside staff rooms.

5. Security of staff mobile devices

Staff must take all sensible measures to prevent unauthorised access to their mobile devices, including but not limited to the use of a PIN, pattern or password to be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time. Staff must never attempt to bypass any security controls in nursery systems or others' own devices.
Staff must ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up-to-date.

6. Compliance with Data Protection Policy

Staff compliance with this BYOD policy is an important part of the nurseries' compliance with the Data Protection laws. Staff must apply this BYOD policy consistently.

7. Support

The nursery conducts annual PAT test on nursery devices and equipment. We request staff/ visitors to bring in any equipment or devices that will be used on site. It then becomes the responsibility of each individual to bring in their equipment on the days set out so they can be tested along with school devices. This includes chargers. Staff may not bring untested items on to nursery property unless they are under one year old and they have proof of this. We will notify staff in advance of the date for PAT testing.

8. Compliance, Sanctions and Disciplinary Matters for staff

Non-compliance of this policy exposes both staff and the nurseries to risks. If a breach of this policy occurs the nursery may discipline staff in line with the school's disciplinary procedure.

9. Incidents and Response

The nurseries take any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of a mobile device should be reported to the SMT in the first instance. Data protection incidents should be reported immediately to the SMT.

Reviewed by: Lucy Meyer
Review date: October 1st 2025

I confirm I have read, understood and agree to adhere to this policy at all times…

Staff member name:_____ signature_____ date_____

SMT name:_____ signature_____ date_____